

ORIGINAL

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

RECEIVED

FEB 10 1994

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of

)

)

)

)

CC Docket No. 93-292

Policies and Rules Concerning
Toll Fraud

REPLY COMMENTS

MCI TELECOMMUNICATIONS CORPORATION

Mary J. Sisak
Donald J. Elardo
1801 Pennsylvania Avenue N.W.
Washington, D.C. 20006
(202) 887-2605

Dated: February 10, 1994

Its Attorneys

No. of Copies rec'd
List ABCDE

0+4

TABLE OF CONTENTS

	<u>PAGE</u>
SUMMARY	i
I. INTRODUCTION	1
II. PBX FRAUD	2
III. PAYPHONE FRAUD	7
IV. LIDB	11
V. CELLULAR	14
VI. CONCLUSION	15
ATTACHMENTS	

SUMMARY

Concerns regarding fraud are reflected in an array of initial comments filed in this proceeding. Most parties agree that accountability for telecommunications fraud must reside in the person or entity controlling, or possessing the ability to control, the environment in which fraud occurs. The element of "control" is thus the linchpin from which all responsibility for fraud must flow.

Any other determination -- such as one that would have all entities involved in telecommunications somehow "share" the fraud risk -- defies logic, precedent and equitable considerations, and would likely have the perverse effect of removing fraud responsibility from those able to prevent it and placing it in those unable to do so. This would be an inappropriate approach, both as a matter of law and policy.

378

BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of)	
Polices and Rules)	CC Docket No. 93-292
Concerning Toll Fraud)	

REPLY COMMENTS

MCI Telecommunications Corporation (MCI) hereby replies to initial comments submitted in response to the Commission's Notice of Proposed Rulemaking (NPRM) in the above-captioned proceeding.¹

I. INTRODUCTION

In its original comments, MCI demonstrated that, to prevent or reduce toll fraud, the Commission should hold accountable for fraud the person or entity that controls, or has the ability to control, the equipment and/or facilities through which fraud originates. In the case of customer premises equipment (CPE) fraud, which includes PBX and private payphone fraud, that person is the telecommunications user. MCI also demonstrated that carrier monitoring of customer traffic cannot prevent fraud; at best, it can only show that fraud has occurred or, perhaps, may be occurring.

MCI demonstrated that users should not be insulated from

¹ MCI's failure to address the comments of any party should not be viewed as either agreement or disagreement with positions reflected in those comments.

fraud responsibility because such insulation and would shift fraud costs to others, and would eliminate user incentives to take steps that are within their control and necessary to minimize or prevent fraud. In addition, because users are in the best position to prevent fraud, their education is extremely important to ensure that they acquire the knowledge necessary to combat fraud successfully. As demonstrated below, the comments filed herein overwhelmingly support MCI's positions.

II. PBX FRAUD

The comments overwhelmingly demonstrate that a PBX user controls, or has the ability to control, its PBX and, therefore, the PBX user is in the best position to prevent fraud involving its PBX.² For example, PBX users program (or can program) their PBXes to eliminate features that allow for unauthorized access to carrier services. In addition, PBX equipment has features which allow users to monitor their traffic and thereby ascertain whether unauthorized calls are

² See Comments of AT&T at 3; WilTel at 2; Telecommunications Resellers Association at 5; Ericsson Corporation at 3-4; Northern Telecom at 2; Competitive Telecommunications Association (CompTel) at 2; Southwestern Bell Corporation (SWB) at 3; NYNEX at 17; and United States Telephone Association at 3.

being made.³ Furthermore, there are many suppliers of fraud detection and monitoring equipment whose equipment can be obtained and used with PBXes.⁴ There are businesses that provide fraud services, such as programming, maintenance and traffic monitoring, to PBX users.⁵ Finally, a number of carriers offer monitoring services that can be used to complement PBX user fraud detection and prevention programs.⁶

A number of PBX users claim that available fraud programs and equipment are too costly.⁷ In addition, they allege that their "destiny" with respect to fraud, is in part "controlled by" the "information, services and equipment" provided by local exchange carriers (LECs), interexchange carriers (IXCs) and CPE providers.⁸ Therefore, these entities should have the legal obligation to warn customers about fraud and, further,

³ See, Comments of Ericsson at 3; and Northern Telecom at 2.

⁴ In addition to record information in this proceeding, trade publications such as Infosecurity News list companies that provide fraud detection and prevention equipment and services.

⁵ For example, TeleDesign states that it manages CPE systems and provides a security audit service.

⁶ See Comments of AT&T at 11; Southern New England Telephone at 5; and Sprint at 4.

⁷ See, the form letter submitted by numerous PBX users.

⁸ Id.

share in the financial responsibility for fraud.⁹

As an initial matter, whether available fraud detection equipment and services are "too costly" is a subjective determination. However, as the attached price lists from XIOX and MicroFrame, two manufacturers of fraud detection equipment, demonstrate, the price of fraud detection and monitoring equipment is not substantial -- especially when one weighs the potential costs associated with fraud incidents. Moreover, contrary to some allegations, MCI's fraud detection program, called MCI Detectsm, currently is provided at no additional charge and, apparently the basic monitoring options provided by Sprint and AT&T are provided at no additional charge as well.¹⁰

In addition, although some PBX users allege that IXCs have a duty to provide "warnings" about fraud, they offer no evidence of carrier neglect in this regard. To the contrary, the comments demonstrate that carriers have undertaken, on a voluntary basis, extensive customer education programs concerning PBX fraud.¹¹ For example, carriers publish and

⁹ Id.

¹⁰ See, Comments of AT&T at 14; and Sprint at 3.

¹¹ See, Comments of AT&T at 3; Sprint at 4; and MCI at 3-4. In addition, LECs have undertaken extensive customer education programs. See, comments of Pacific Bell and Nevada Bell (PacBell) at 12; NYNEX at 4; and Ameritech at 2.

distribute, free-of-charge, pamphlets and periodic newsletters, hold seminars, and staff fraud "hot lines," among other things, to educate customers about PBX fraud.¹² In any event, it is indisputable that services provided by carriers are not the cause of PBX fraud. Rather, fraud results from the compromise of PBX equipment interconnected to the public switched network, which connection provides access to IXC services.

It appears from the comments that the primary complaint of PBX users is that equipment providers have not furnished the appropriate information concerning the capabilities and potential abuses of their products.¹³ Some manufacturers, such as Northern Telecom, state that they have begun to provide such information in their equipment manuals. However, these recent efforts may not reach PBX users with older vintage equipment. Therefore, to the extent possible, equipment manufacturers should provide fraud information to PBX users with older equipment as well.

In addition, the comments demonstrate that the various means of detecting and preventing fraud, when applied, are effective. For example, USL Capital states that, since it

¹² Carriers voluntarily undertake these measures in part to preserve the customer relationship because when fraud does occur, there can follow a period of contention between the carrier and the customer.

¹³ See, the form letter submitted by numerous PBX users.

implemented measures to prevent fraud, no unauthorized persons have been able to successfully infiltrate its PBX.¹⁴ In addition, RAK Associates, a telecommunications consulting firm, states that no system which it has designed, installed and administered has been penetrated by a successful toll fraud attempt.¹⁵

Thus, it is clear from the record that PBX users have many effective options available to them to combat fraud. It is equally clear, however, that some PBX users do not wish to pay to implement available options and, moreover, do not wish to be held accountable for any fraud that results. The Commission must reject this position because, first, it is the user's decision to purchase or lease a PBX and, second, it is within the user's exclusive control to take measures to deter or prevent PBX fraud. Therefore, any fraud that results because of these user decisions must be viewed as the responsibility of the PBX user.

To apportion financial responsibility in these cases would be fundamentally unfair and contrary to the public interest because entities and individuals without control over decisions proximately resulting in fraud would have to pay for it. Thus, customers who made the efforts and incurred the

¹⁴ USL Capital Comments at 1.

¹⁵ RAK Associates Comments at 1.

costs to address and avoid fraud ultimately would be forced to share the costs of fraud with their less diligent counterparts through higher rates and charges.

In addition, by reducing the potential financial impact of fraud upon PBX users, the Commission would be changing the financial risks and benefits associated with implementing fraud prevention and detection measures. By apportioning financial responsibility, the Commission actually would be encouraging PBX users not to implement fraud detection and prevention measures and, as a result, more fraud likely would result. Clearly, such a result would not be in the public interest.

III. PAYPHONE FRAUD

The comments also demonstrate that private payphone owners (PPOs) are in the best position to address and avoid fraud originating at their equipment. Each PPO makes the decision to place its equipment at a particular location and to provide access to the public switched network at that location by inviting members of the public to use the equipment.¹⁶ The PPO alone selects the type of phone to install, including all features and functions thereof, as well as telecom services and features connected to the phone. (As

¹⁶ See, Comments of American Public Communications Council (APCC) at 1.

the comments demonstrate, PPOs that install "smart" payphones can program those phones to prevent certain types of calls and, thus, control fraud.)¹⁷ The PPO has the ability to secure the telephone line between the phone and the LEC demarcation point. The PPO alone selects whether to subscribe to "payphone service" and whether to purchase originating line screening (OLS), billed number screening (BNS) and international blocking (IDDB) from the LEC.

Although the PPOs admit there are safeguards that can be taken to secure their equipment, they argue that the responsibility for preventing toll fraud should rest with carriers. As examples of measures carriers could take to prevent payphone fraud, the PPOs state that the LECs should offer OLS, BNS and IDDB;¹⁸ IDDB should include blocking of the 809 area code;¹⁹ the LECs should make available safeguards against secondary dial tone or dial tone reoriginations;²⁰ the LECs should be required to do more to secure the network

¹⁷ See, Comments of APCC at 2; and Florida Pay Telephone Association at 4.

¹⁸ See, Comments of APCC at 18; and Florida Pay Telephone Association at 3.

¹⁹ See, Comments of APCC at 20; Florida Pay Telephone Association at 12; and Independent Payphone Association of New York at 16.

²⁰ See, Comments of APCC at 21.

interface;²¹ and the LECs should assign 8000 and 9000 numbers to payphones so that international operators can identify a payphone and not complete collect calls to the phone.²²

The PPOs argue that IXCs should be required to monitor payphone traffic and report any "unusual" traffic to the PPO.²³ The American Public Communications Council (APCC) argues that a carrier that fails to provide "adequate fraud monitoring" should not be allowed to hold the PPO liable for fraudulent charges even if the PPO does not subscribe to blocking and screening services.²⁴ In effect, they seek to make carriers "insurers" of their business undertakings.

It is clear from the PPOs' admissions that there are a number of measures, in addition to purchasing OLS and BNS, that they could take to prevent fraud. Given this and the fact that the environment in which they locate their equipment is exclusively within their choice and control, financial responsibility for payphone fraud must reside with the PPOs.

It is also clear that there are a number of services that the LECs provide, and services which the PPOs believe the LECs should provide, to assist PPOs in preventing fraud. To the

²¹ See, Comments of APCC at 21.

²² See, Comments of APCC at 22.

²³ See Comments APCC at 22; and New Jersey Payphone Association at 2.

²⁴ APCC Comments at 23.

extent that these services fail, LECs should be financially responsible for the resulting fraud.

What has not been demonstrated is why IXCs should be held financially responsible for payphone fraud. Although the PPOs argue that IXCs should provide monitoring services, monitoring does not prevent fraud -- at best it may indicate that fraud has occurred. Moreover, in the payphone environment, where the phone is being used by transient users and members of the public, the PPOs have failed to demonstrate how an IXC could even begin to determine whether a particular calling pattern is "unusual" and, thus warn a PPO of suspected fraud.

In addition, as shown by MCI in its comments, there is no contractual relationship between the IXC and PPO in connection with the provision of OLS, BNS and IDDB services. Moreover, the comments indicate that when these services fail, failure is usually caused by LEC error.²⁵ Accordingly, it would be fundamentally unfair to place any financial responsibility for payphone fraud that results from a failure of these services on IXCs.

Also clear from the comments is that the PPOs' primary goal is not to prevent fraud, but to eliminate their financial responsibility for fraud. Thus, APCC urges the Commission to

²⁵ The Independent Payphone Association of New York states that the failure of LEC blocking and screening services is almost always due to LEC error or negligence. Comments at 10.

clearly define the measures that a PPO must take "to avoid liability."²⁶ The clear indication is that if the Commission adopts the Florida Commission proposal and requires PPOs to purchase OLS and BNS to avoid liability for fraud, PPOs will do no more to combat fraud - even though there are many other steps that could be taken to do so. Moreover, the result will be the same as in Florida -- namely, the number of fraud complaints at the Commission may decrease,²⁷ but the incidence of fraud will not.²⁸ On the contrary, if the PPOs are permitted to become less diligent in securing their equipment, it is likely that the incidence of payphone fraud will increase. Clearly, such a result would not be in the public interest.

IV. LIDB

LECs argue that in order to be able to monitor card calls and detect fraudulent calling patterns, IXC's should be

²⁶ APCC Comments at 10.

²⁷ The Florida Pay Telephone Association states that there have been no civil or administrative proceedings regarding fraudulent toll calls at payphones since the adoption of the Florida rules. Comments at 1-2.

²⁸ GTE states that while the number of complaints filed at the Florida Commission concerning toll fraud has decreased, the amount of fraud has not decreased. Comments at 11.

required to query LIDB for every call²⁹ and to provide originating and terminating ANI to the LEC.³⁰ The LECs also argue that IXCs should not be able to charge for the provision of ANI information because it would be provided to prevent toll fraud.³¹ Finally, some LECs argue that they should not be liable for card fraud because they cannot prevent it.³²

MCI does not object to providing originating and terminating ANI to LECs for fraud detection if the LECs are willing to assume the financial risk for any fraud that occurs. This is an equitable compromise, given that a) the card is issued by the LEC to its customer; b) the LEC charges the IXC for the LIDB dip; and c) with the originating and terminating ANI for all calls carried over all IXC networks, the LEC will be the only entity with complete visibility into all calling with its card. Thus, under the Commission's standard, the LEC would be in the best position to control fraud.

Currently, there is no need for MCI to provide

²⁹ See, Comments of SWB at 11; NYNEX at 25; and PacBell at 17.

³⁰ See, Comments of SWB at 11; NYNEX at 25; PacBell at 17; US West at 22; Ameritech at 5; BellSouth at 12; and Bell Atlantic at 8.

³¹ See, Comments of SWB at 12; and BellSouth at 12.

³² See, Comments of SWB at 12; PacBell at 18; and Ameritech at 5.

originating and terminating ANI to LECs in order for the LECs to reduce their fraud exposure in connection with calls carried by MCI because, as between MCI and the LECs, the LECs do not assume financial responsibility for fraudulent calls. The LECs may have a need for this information, however, to reduce their fraud exposure with respect to calls carried by AT&T because, it appears, the LECs assume some responsibility for fraudulent calls that AT&T carries through "Mutual Honoring Agreements."³³ Some LECs, however, do not want to assume any financial liability for card calls carried by other IXCs even if they receive originating and terminating ANI for the calls. The result of all this -- if the Commission accepts the LEC proposals -- would be that IXCs (other than AT&T) will incur greater costs because of additional LIDB queries, and they will incur costs in connection with their provision of originating and terminating ANI -- but their fraud exposure would remain unchanged. Clearly, this is an inequitable result with serious anti-competitive overtones.

The LECs also appear to want IXCs to provide originating and terminating ANI so that they can develop and market new products.³⁴ In addition, such information could be used by the LECs to market interLATA services if they were allowed

³³ CompTel Comments at 7.

³⁴ See, Comments of BellSouth at 12; and Bell Atlantic at 9.

entry into this market.

Therefore, at a minimum, in order to ensure that the LECs do not gain competitive advantages in the name of "fraud prevention", the Commission should only require IXCs to provide the originating and terminating NPA-NXX as distinct from the entire number. As demonstrated by the Interexchange Carrier Industry Committee Toll Fraud Subcommittee (ICIC), this information is sufficient to allow the LECs to perform fraud monitoring.³⁵ In addition, the Commission should prohibit the LECs from using this information for any purpose other than fraud monitoring.

Finally, the Commission should re-evaluate whether LECs should be allowed to charge for LIDB queries since the resulting information is used by IXCs to control toll fraud.³⁶ At a minimum, the Commission should initiate an investigation under Section 205 of the Act to determine whether the LECs' LIDB rates are reasonable in order to ensure that they are not unjustifiably profiting from a fraud control mechanism.

V. CELLULAR

The Commission should reject the argument of some

³⁵ See, Comments of the ICIC at 15.

³⁶ To maintain equity and symmetry of regulation, the LECs should not be able to charge for LIDB queries if IXCs are not permitted, in turn, to charge for ANI delivery.

cellular carriers that IXCs should be responsible for toll charges associated with fraudulent calls, where cellular carriers provide equal access.³⁷ According to the cellular carriers, IXCs have the ability to monitor and prevent such calls and, therefore, the IXCs should be responsible for toll charges resulting from fraud.

This simply is not true. As demonstrated by MCI in its comments, monitoring does not prevent fraud -- at best, it may indicate that fraud has occurred or may be occurring. Moreover, many cellular providers do not pass information digits to the IXC and, therefore, the IXC cannot even identify the call as a cellular call.

In any event, the IXCs have no capability to determine whether a call presented from a cellular carrier's network is originating from an authorized cellular phone. Rather, cellular carriers must design their networks to prevent unauthorized use. Accordingly, they should be financially responsible for any fraudulent toll charges that result from the failure of their networks.

VI. CONCLUSION

Based on the foregoing and MCI's original comments, MCI

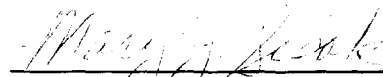
³⁷ See, Comments of Cellular Telecommunications Industry Association at 13; and McCaw Cellular Communications, Inc. at 7.

respectfully urges the Commission to adopt the positions set forth by MCI in any rules it may propose.

Respectfully submitted,

MCI Telecommunications Corporation

By:



Mary J. Sisak
Donald J. Elardo
1801 Pennsylvania Avenue, N.W.
Washington, D.C. 20006

Dated: February 10, 1994

ATTACHMENT A

PRODUCT	SUGGESTED RETAIL PRICE
---------	---------------------------

MAINTENANCE PORT
PROTECTION

Xiox Hacker Deadbolt™

XHDB-I D3 (requires an XHP A2 or larger) security options include AT&T tested suitable, second password to pagers, and call out for permission features	\$995
---	-------

XHDB-E D1 standalone	\$1295
----------------------	--------

XHDB-I D4 (requires an XHP A2 or larger) protects 2 ports; i.e., PBX and Voice Mail	\$1495
---	--------

XHDB- E D2 standalone, protects 2 ports; i.e., PBX and Voice Mail	\$1995
--	--------

XHDB- E D3 standalone, including AT&T tested suitable, second password to pagers, and call out for permission features	\$2995
---	--------

XHDB- E D4 standalone, protects 2 ports; i.e., PBX and Voice Mail, including AT&T tested suitable, second password to pagers, and call out for permission features	\$3695
--	--------

January 31, 1994

PRODUCT	SUGGESTED RETAIL PRICE
---------	---------------------------

REACTIVE, DIAGNOSTIC
SYSTEMS

Xiox Hacker Tracker™	\$2195
----------------------	--------

GBS Plus Xplorer, full call accounting system for up to 500 extensions including software, rate table, call storage buffer, Product Support, Warranty, and built-in XHT	\$3095
---	--------

GBS Plus Bundle 200, full call accounting system for up to 200 extensions including software, rate tables, call storage buffer, Product Support, Warranty, built-in XHT; and the advanced features of Custom Reporting, Repricing, and Reorganization	\$5695
---	--------

GBS Xplorer 2, same as the Xplorer, except the extension limit is 1000	\$7495
--	--------

GBS Plus Bundle 500, same as GBS Plus Bundle 200, except the extension limit is 500	\$9195
---	--------

GBS Plus Bundle 1000, same as GBS Plus Bundle 1000, except the extension limit is 1000	\$14,095
--	----------

GBS Plus Bundle 2000, same as GBS Plus Bundle 2000, except the extension limit is 2000	\$16695
--	---------

January 31, 1994

PRODUCT	SUGGESTED RETAIL PRICE
---------	---------------------------

PREVENTATIVE, WARRANTED SOLUTIONS	
--------------------------------------	--

Xiox Hacker Preventer™	
------------------------	--

XHP Model A artificial intelligence, and voice password analysis for up to approximately 300 users for applications involving voice mail, automated attendants, voice response units, teleconferencing bridges, modem pools, LAN connections, and IRISA™ (Intelligently Restricted Inward System Access)- Xiox' warranted replacement for DISA or Remote Access.	\$6995
--	--------

XHP Model A2 approximately 800 users	\$9995
---	--------

XHP Model B approximately 1400 users	\$12995
---	---------

XHP Model C approximately 4200 users	\$15995
---	---------

XHP Model D approximately 5000 users	\$21995
---	---------

XHP Model E approximately 10000 users	\$27995
--	---------

January 31, 1994

ATTACHMENT B

MicroFrame User Price List

Doc. No. 30804.1430

Effective: August 1, 1993

Port Security & Alarm Management Systems

<i>Secure Sentinel</i> IPC Series "Fully Programmable" Intelligent Port Controllers											
Model No.	# Int. Modems	# RS-232 Ports	14.4kbps Modem *	1MB Memory *	48V DC Power	Holdover Battery	Security Mgr	Alarm Mgr	CDR Mgr **	Environ. Mgr**	List Price
IPC-104	0	4	n/a	n/a	opt	opt	std	std	n/a	opt	\$ 1,250
IPC-200	1	1	opt	n/a	opt	opt	std	std	n/a	opt	\$ 1,250
IPC-300	1	2	opt	n/a	opt	opt	std	std	n/a	opt	\$ 1,450
IPC-400	2	4	opt	n/a	opt	opt	std	std	n/a	n/a	\$ 1,950
IPC-500	1	6	opt	n/a	opt	opt	std	std	n/a	n/a	\$ 1,950
IPC-310	1	2	opt	std	opt	opt	std	std	std	opt	\$ 2,495
IPC-410	2	4	opt	std	opt	opt	std	std	std	n/a	\$ 2,995
IPC-510	1	6	opt	std	opt	opt	std	std	std	n/a	\$ 2,995
<i>Dial Port Sentry</i> Single-Port Security Management Systems											
DPS-102	0	2	n/a	n/a	n/a	n/a	std	n/a	n/a	n/a	\$ 795
DPS-104	0	4	n/a	n/a	n/a	n/a	std	n/a	n/a	n/a	\$ 995
DPS-200	1	1	n/a	n/a	n/a	n/a	std	n/a	n/a	n/a	\$ 995

* Factory Installed Option

** Requires 1MB Memory Option

Model No.	<i>Available Options</i>	List Price
IPC-XXX F	14.4kbps Internal Modem	\$ 250
IPC-XXX R	Real World Interface Board (for use with Environmental Management Application)	\$ 380
DCC-1	Dual Contact Closure Input	\$ 70
BBU-12	Battery Back-Up Unit	\$ 125
BBU-48	48VDC Power Supply with Battery Back-Up	\$ 225
EMC-1	Environmental Management Application Program (Requires Real World Interface Board)	\$ 250